CCTV Policy

CCTV Policy

1 Introduction

1.1 The purpose of this policy is to regulate the management, operation and use of CCTV systems (Closed Circuit Television) at each of the Trust schools/academy's.

1.2 Cameras are located in and around the school/academy sites. All cameras are monitored by either the Senior Site Facilities Maintenance Officer or System Manager and images are only available to selected senior staff:

1.3 This policy follows General Data Protection Regulation (GDPR) 2016.

1.4 The policy will be subject to review bi-annually to include consultation as appropriate with interested parties.

2 Objectives of the CCTV System

2.1 To protect students, staff and visitors

2.2 To increase personal safety and reduce the fear of crime.

2.3 To protect the Trust school/academy buildings and assets.

2.4 To support the Police in preventing and detecting crime.

2.5 To assist in identifying, apprehending and prosecuting offenders.

2.6 To assist in managing the school/academy.

3 Statement of Intent

3.1 The CCTV system will seek to comply with the requirements both of the GDPR and the Commissioner's Code of Practice.

3.2 The school/academy will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under GDPR.

3.3 Cameras will be used to monitor activities within the school/academy and its grounds to identify criminal activity actually occurring, anticipated, or perceived. They will be used for securing the safety and wellbeing of the students, staff and school/academy visitors.

3.4 The system is designed to deny observation on adjacent private homes, gardens and other areas of private property.

3.5 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

3.6 Images will only be released to the media for use in the investigation of a specific crime with the written authority of the Police.

3.7 Images will never be released to the media for purposes of entertainment.

3.8 The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover of detect every single incident taking place in the areas of coverage.

3.9 Warning signs, as required by the Code of Practice of the Information Commissioner are clearly visible on the site.

4. System Management

4.1 The system will be administered and managed by the Chief Operating Officer of the Constellation Trust, who will act as the Data Controller in accordance with the principles and objectives expressed in the policy

4.2 The day-to-day management will be the responsibility of both the Head of School and the Site Facilities Maintenance Officer, who will act as the System Manager.

4.3 The system and the data collected will only be available to the Data Controller, the Head of School and the System Manager.

4.4 The CCTV system will be operated 24 hours each day, every day of the year.

4.5 The System Manager will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

4.6 Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

4.7 The System Manager must satisfy himself/herself of the identity of any person wishing to view images or access the system and, the legitimacy of the request. Access will be refused, where any doubt exists.

4.8 Details of all visits and visitors will be recorded in the system logbook including: time/data of access and details of images viewed.

4.9 Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

5. Liaison

5.1 Liaison meetings may be held with all bodies involved in the support of the system.

6. Download Media Procedures

6.1 In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any downloaded media used to record events from the hard drive, must be prepared in accordance with the following procedures:

6.1.1 Each download media must be identified by a unique mark and ideally should be saved to a cloud based solution or an encrypted USB.

6.1.2 Before use, each download media must be cleaned of any previous recording.

6.1.3 The System Manager will register the date and time of download media insertion, including its reference.

6.1.4 Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If downloaded media is not copied for the Police before it is sealed, a copy may be made at a later date, providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.

6.1.5 If downloaded media is archived the reference must be noted.

6.2 Images may be viewed by the Police for the prevention and detection of crime and by authorised North Eastern Education and Library Board (NEELB) Officers.

6.3 A record will be maintained of the release of any downloaded media to the Police or other authorised applicants

6.4 Viewing of images by the Police must be recorded in writing

6.5 Should images be required as evidence, a copy may be released to the Police under the procedures described in this policy. Images will only be released to the Police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the school/academy, and download media (and any images contained thereon) are to be treated in accordance with GDPR. The school/academy also retain the right to refuse permission for the Police to pass the downloaded media (and any images contained thereon) to any other person. On occasions, when a Court require the release of downloaded media this will be produced from the secure evidence store, complete in its sealed bag.

6.6 The Police may require the school/academy to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the Police

6.7 Applications received from outside bodies (e.g. Solicitors) to view or release images will be referred to the North Eastern Education & Library Board (NEELB), Legal Department.

7.0 Assessment of the System and Code of Practice

7.1 Performance monitoring including random operating checks may be carried out by the Head of School or the Data Controller.

8.0 Complaints

8.1 Any complaints in relation to the school/academy's CCTV system should be addressed to the Head of School.

9. Access by the Data Subject

9.1 The GDPR provides Data Subjects (individuals to whom 'personal data' relate) with a right to data held about themselves, including those obtained by CCTV.

9.2 Requests for Data Subject Access should be made to the NEELB, Legal Department.

10. Public Information

10.1 Printed copies of this policy will be available to the public from the school/academy reception.

11.0 Summary of Key Points

11.1 This policy will be reviewed every two years.

11.2 The CCTV systems are owned and operated by the schools/academy's.

11.3 The CCTV system and images are not available to visitors except under circumstances as outlined in this policy.

11.4 Liaison meetings may be held with the Police and other bodies if required.

11.5 Downloaded media will be used properly, indexed, stored and destroyed after appropriate use, in accordance with GDPR.

11.6 Images may only be viewed by authorised personnel, the school/academy, NEELB Officers and the Police.

11.7 Downloaded media required as evidence will be properly recorded onto an encrypted device, witnessed and packaged before copies are released to the Police.

11.8 Downloaded media will not be made available to the media for commercial or entertainment purposes.

Appendix 1

European Data Protection Law
(General Data Protection Regulation 2016)

1 References Information

1.1 https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/. UK General Data Protection Regulations (UKGDPR)

1.2 The Guide to the GDPR explains the provisions of the GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection.

1.3 The GDPR forms part of the data protection regime in the United Kingdom, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this apply, like the GDPR, from 25 May 2018.